



Systems Engineering Facility (SEF)

Concept of Operations Document

Release Version 1.2

November 19, 2009

Abstract

This Concept of Operations Document outlines the current Systems Engineering Facility operations as well as a conceptual model for future operational enhancements. This document was authored in direct response to SR # 2007-0000030 and SAE (Special Area of Emphasis) # 5: (SEF Operational Model) for the period that ends May 31st, 2008. This document has been updated in direct response to SR 2009-0000846 Innovations Lab

Preface

The purpose of this document is to provide a framework for operating and managing the Systems Engineering Facility (SEF). To this end, this document will be considered a living document, updated as necessary, throughout the lifecycle of the facility to allow for changes in direction or requirements. The information within this document was generated by the HITSS Engineering team with substantial input from other HITSS departments. It should be noted that the basic operational requirements for the SEF are dictated in the HITSS contract Statement of Work (SOW) Task Order 10.01.

Table of Contents

Abstract.....	2
Preface.....	3
1. Scope.....	8
1.1 Introduction.....	8
1.2 Identification.....	8
1.3 Document Overview	8
1.4 Document Organization.....	8
2. Referenced Documents	9
3. Systems Engineering Facility	9
3.1 SEF Operational Policies and Constraints	9
3.2 Current Facility	9
3.3 Current SEF Services and Support Functions.....	9
3.4 SEF Metrics	10
4. SEF Architecture.....	11
4.1 Facility Overview.....	11
4.2 SEF Network Overview	12
5. SEF Inventory	15
5.1 Inventory Maintenance	15
5.2 Logistical Support.....	15
6. SEF Operations, Procedures and Testing.....	16
6.1 SEF Operations, Scheduling and Resource Management.....	16
6.1.1 Scheduling and SEF Availability.....	17
6.1.2 Test Request Process.....	17
6.1.3 Test Plan Process	18

6.1.4	Developer and Government Testing	18
6.1.5	Test Completion and Documentation	18
6.1.6	Innovation and Prototype Lab.....	19
6.2	Lifecycle of SEF (Hardware) Assets	20
6.2.1	Semi-Permanent Assets	20
6.2.2	Transitory Assets	21
6.2.3	Asset Life Cycle Conclusion	21
6.3	SEF Server and Workstation Refreshes.....	21
6.3.1	Workstation (ODIN) Refresh Process	21
6.3.2	SEF Server Refresh Process.....	21
6.3.2.1	JumpStart Service	22
6.3.2.2	Kickstart Service.....	22
6.4	SEF System Backup and Recovery.....	22
6.5	System Migration from the SEF to the NHCC	22
6.6	Phase-out or Retirement of SEF Hardware.....	23
6.7	SEF Configuration Management	23
6.7.1	SEF System Update Management	23
6.7.1.1	Windows Updates	23
6.7.1.2	Solaris Updates	24
6.7.1.3	RedHat Linux Updates.....	24
6.7.1.4	Macintosh Updates.....	24
7.	Security Controls in the SEF.....	24
7.1	System Security Application Software	25
7.1.1	Security Policies.....	25
7.2	Production Data and Removal Process	25

7.3 PII / Privacy Data.....	26
8. SEF Manager Roles and Responsibilities	26
8.1 SEF Manager	26
8.2 SEF Manager Core Skill Requirements	27
8.3 SEF Users.....	27
9. Recommendations.....	27
9.1 Process Improvement.....	28
9.2 Network Address Translation (NAT)	28
9.3 Developer Access.....	28
9.4 Automated Patch Management	28
9.5 Research Bug Tracking Systems	28
9.6 Develop Web Log for SEF CM Tracking.....	28
9.7 Reorganize SEF Server Racks	28
Appendix A: SEF Patch Panel and Switch Layout.....	29
Appendix B: SEF Hardware Assets	30
Appendix C: System Engineering Facility (SEF) Work Request Form	34
Appendix D: SEF Test Request Process.....	35
Appendix E: Acronyms and Abbreviations	36

List of Figures

Figure 1: SEF Floor Plan.....	12
Figure 2: SEF Network Diagram.....	13
Figure 3: Ethernet Cabling Scheme.....	14

List of Tables

Table 1: SEF Services and Support Functions.....	9
Table 2: SEF Metrics.....	10
Table 3: ODIN Workstations.....	16
Table 4: SEF Security Boundaries.....	23

1. Scope

The scope of this document is to provide a comprehensive representation of the operational processes of the Systems Engineering Facility and the facility's relationships with other organizations.

1.1 Introduction

The mission of the Systems Engineering Facility (SEF) is to protect the NASA Headquarters production environment by providing a controlled setting and location for the testing, evaluation, and mitigation of issues related to deploying new applications, software, hardware, and systems as well as an environment for testing and troubleshooting issues and problems that have been anticipated or identified in the production environment. The SEF serves as a test bed to prove or test for interoperability prior to deployment and a test facility where custom, COTS, and GOTS applications could be tested as well as prototyping, pilot testing, evaluations and exploration of new technology could be conducted. The SEF strives to support the integration of information and processes across programs, NASA Headquarters and NASA Centers as well as support emerging Information Technology needs of the Agency.

1.2 Identification

This Concept of Operations document is a high-level operational description of the NASA Headquarters SEF. This document will be complimented by the Systems Engineering Facility Operations Manual that will provide details and guidelines for the SEF Personnel on proper daily operations of the facility.

1.3 Document Overview

The purpose of this Concept of Operations document is to:

- Define the roles, responsibilities, processes, and procedures necessary to operate the SEF commensurate with the aforementioned scope.
- Discuss the principles and practices underlying the SEF operations such as inventory control, systems management, security and scheduling.

1.4 Document Organization

The layout of the SEF Concept of Operations is largely based on the IEEE Standard 1362-1998 and describes a support process and not a system. *Portions of this document are confidential or business proprietary and not approved for the public.* The remaining document is organized in the following sections:

- Section 2 – lists all documents that have been referenced in this document;
- Section 3 – provides a functional overview of the SEF;
- Section 4 – provides a logistical and physical overview of the SEF;
- Section 5 – provides an overview of logistical support;
- Section 6 – provides an overview of SEF operations, procedures and processes;
- Section 7 – provides an over view of SEF systems security procedures;
- Section 8 – lists the roles and responsibilities of SEF personnel;
- Section 9 – provides recommendations for SEF operations.

2. Referenced Documents

This section lists the documents referenced in this concept of operations document.

- IEEE Std 1362-1998, IEEE Guide for System Definition – Concept of Operations Document, source – <http://standards.ieee.org>
- The governing document for the HITSS contract is the HITSS Statement of Work (SOW) Task Order 10.01. Section 4 Systems Engineering, Integration, Pathfinding and Telecommunications Services, subsection 4.1.11 The Systems Engineering Facility. This section contains the specifics on the contractual requirements of the SEF.

3. Systems Engineering Facility

HITSS Engineering is responsible for the operations and maintenance of the SEF.

3.1 SEF Operational Policies and Constraints

The SEF is governed by the following policies and constraints:

- Applications, products and systems testing requests are scheduled on a first-come first-serve basis except if identified as a high priority which would then be given precedence over other requests for testing. A high priority would be identified by either HITSS, ODIN or NASA management and agreed to by HITSS and NASA management and communicated to the SEF staff.
- Emergency testing requests are those requests with less than 24 hour advance notice. These requests are otherwise similar to high priority requests but require approval of the HITSS engineering manager.
- SEF users need to familiarize themselves with the section(s) of the SEF Concept of Operations document (this document) that are relevant to their work before using the SEF.
- The facility is physically secured after working hours. Access to the facility during this time must be requested and approved in advance.
- The facility must have the proper equipment to run operating systems, applications, databases and other software required for testing.
- Some Mainframe applications can be tested within a test region on the mainframe with the secure 3270 emulator.

3.2 Current Facility

The SEF facility includes hardware, software, operating systems, networking, infrastructure, COTS, GOTS and custom software. All of these, form the basic SEF infrastructure and the foundation for the basis of the SEF concept of operations.

The SEF is located in room CY31 in the NASA Headquarters Computer Center (NHCC) and is physically accessible between the hours of 8:00 am to 4:00 p.m. Access to this facility after hours must be requested and approved in advance. Reasonable effort is made to ensure that the facility is available for those that need access after hours.

3.3 Current SEF Services and Support Functions

Table 1 lists and summarizes the primary services and support functions performed by

the SEF.

Services and Support Functions	Description
Testing Environment Preparation	The SEF prepares the testing environment, allocates resources and coordinates scheduling with the testing requestor.
Hardware Testing	The SEF ensures that the appropriate hardware is available, properly configured and available for testing.
Software Testing	The SEF ensures that the appropriate software such as operating systems, office products and other licensed software are available, and installed for testing.
Applications Testing	The SEF supports applications development with the testing of NASA HQ and Agency-wide applications as well as assisting in the troubleshooting efforts associated with the application.
VoIP	The SEF supports VoIP with testing and troubleshooting.
Innovation Lab and Prototype Testing	The SEF provides personnel, hardware, software and an environment that fosters innovation and prototyping.
AirGap	The SEF supports the AirGap network by assisting operations with network and KVM connections as well as troubleshooting efforts.
Server Hosting	The SEF supports a number of dedicated semi-permanent and pre-production servers for software and applications testing.
Forensic Analysis	The SEF provides support to the Forensic Analysis environment for HITSS IT security.
Vendor Support	The SEF assists external vendors with arranging and preparing for hardware, software, and/or system demonstrations and evaluations.
Ad Hoc Services	The SEF provides additional services such as technical consultations, ODIN triage assistance and customer outreach.

Table 1 – SEF Services and Support Functions

3.4 SEF Metrics

The following metrics are defined for the SEF in the HITSS SOW Task Order 10.01:

	SEF Configuration and Availability
Requirement	Testing shall be conducted in an environment that resembles the environment that the system will be deployed in and coordinated with the requestor. Availability to the SEF shall be provided through scheduling.
Standard	95% of the SEF configurations are appropriate for the applicable testing scenarios and available as scheduled by the requester.
Deliverable(s)	The SEF is available and configured to meet the requestors' requirement(s).
Measurement Method	Customer survey and contractor provided metrics

	SEF Testing
Requirement	Perform testing to determine compatibility with existing environment and provide test support when performing compatibility testing.
Standard	Test all new products for compatibility against the existing environment to avoid post deployment compatibility problems. Provide test support to avoid post deployment compatibility problems.
Deliverable(s)	SEF Test Results Report upon testing completion and SEF test support
Measurement Method	Customer survey and contractor provided metrics

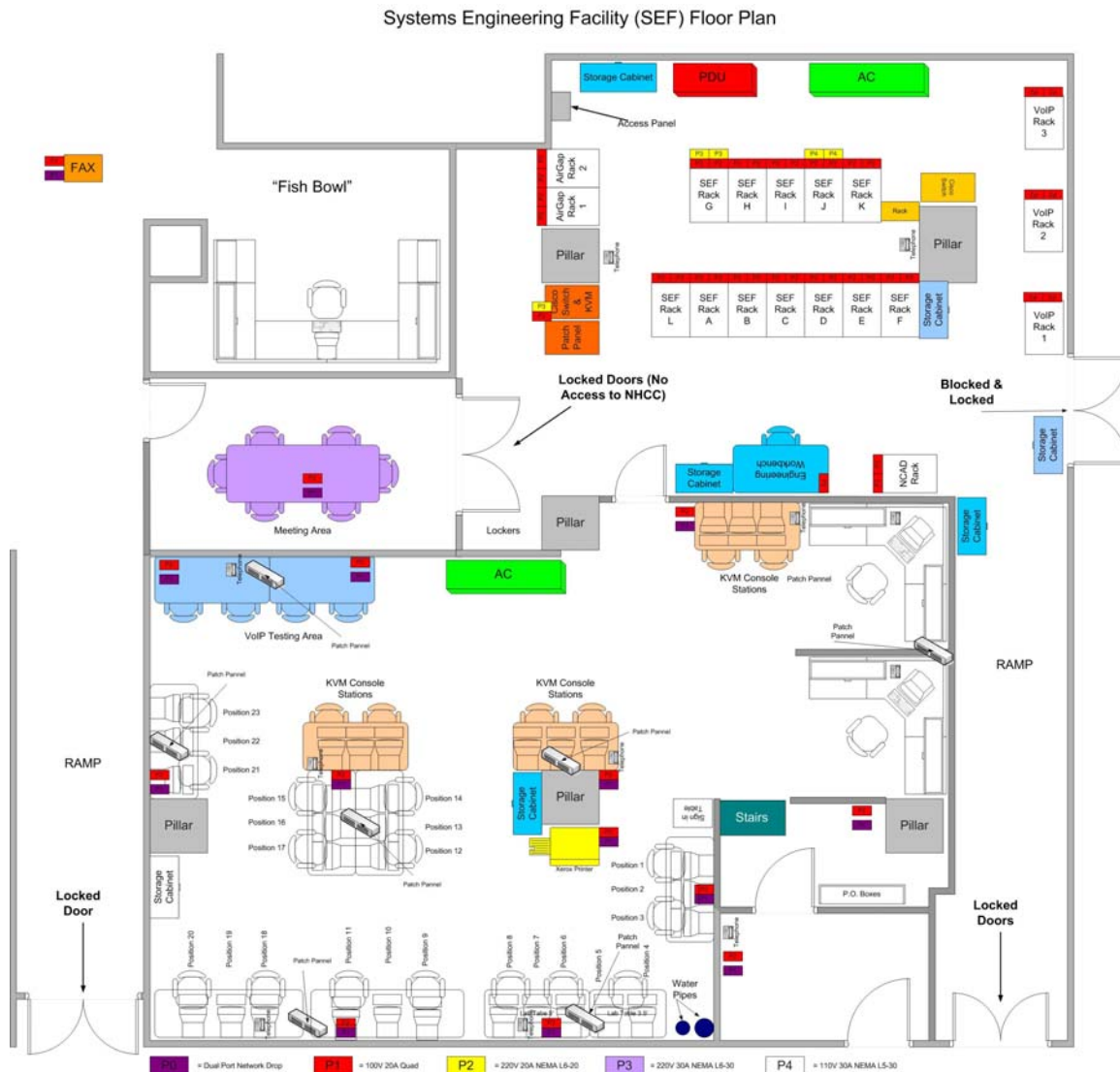
Table 2 – SEF Metrics

4. SEF Architecture

This section provides a logical and physical description of the SEF.

4.1 Facility Overview

The SEF is segregated into two main sections (Figure 1). The SEF user testing area contains workstations, KVM access, and a VoIP testing area. The SEF server area contains equipment racks, SEF servers, networking gear, NCAD, VoIP and AirGap networks.



4.2 SEF Network Overview

The SEF network is composed of multiple Virtual Local Area Networks (VLANs) which are illustrated in Figure 2. The SEF Private VLANs are controlled by a Cisco 6509 switch. This switch also provides the routing between the VLANs.

The SEF public and console networks are implemented using small Cisco switches to ensure physical isolation. Ethernet cables are color-coded to assist in quickly identifying VLAN assignments (Figure 3). Appendix A illustrates the patch panel and primary internetworking devices that facilitate internal and external access to SEF servers and services.

SEF network traffic is controlled by two firewalls, DevGate and Battleship.

The DevGate firewall controls access to and from the SEF private network and the Battleship firewall controls access to and from specific systems on the SEF public network.

Both the DevGate and Battleship firewalls as well as the SEF Cisco 6509 switch are controlled by Network Operations.

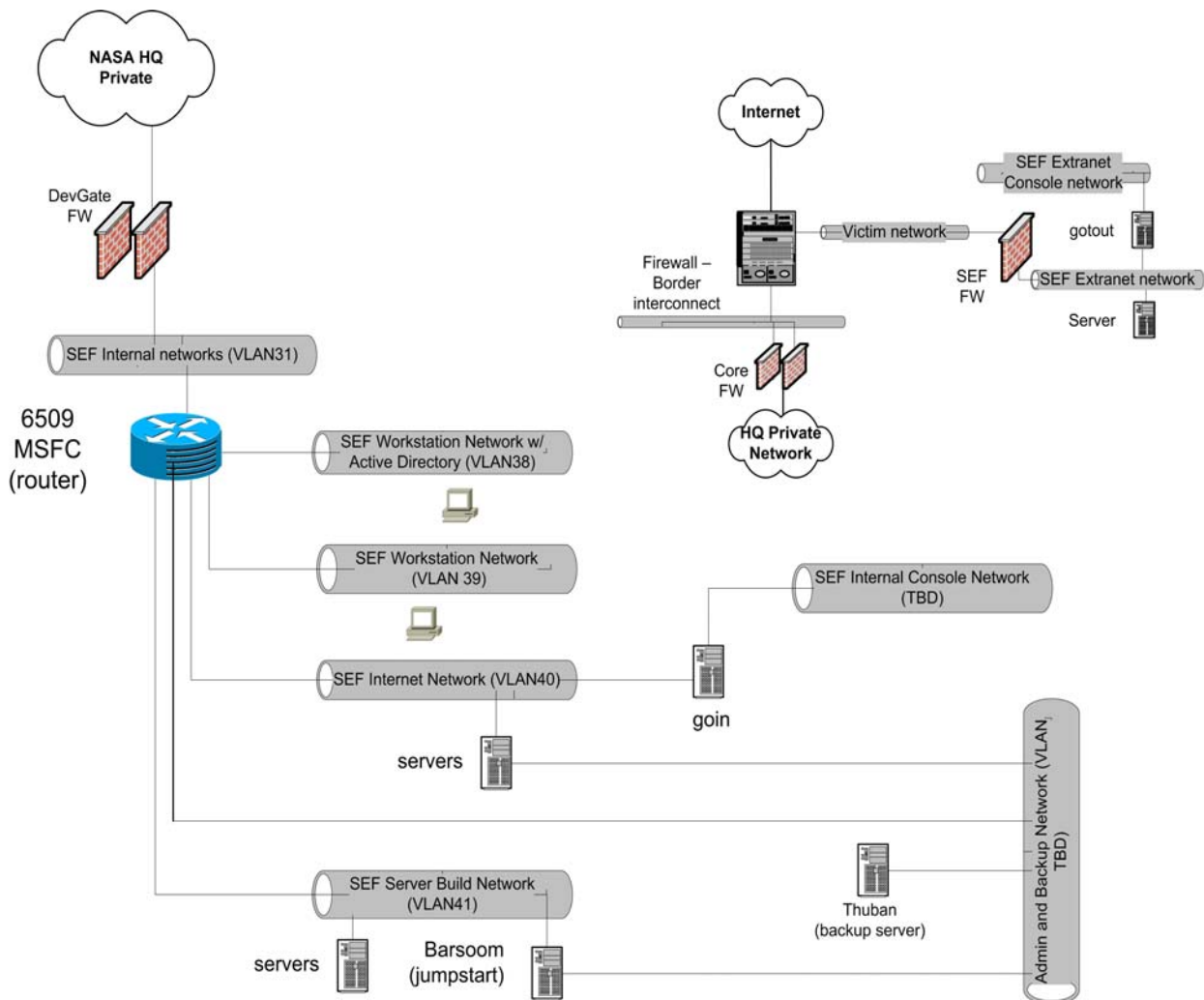


Figure 2 – SEF Network Diagram

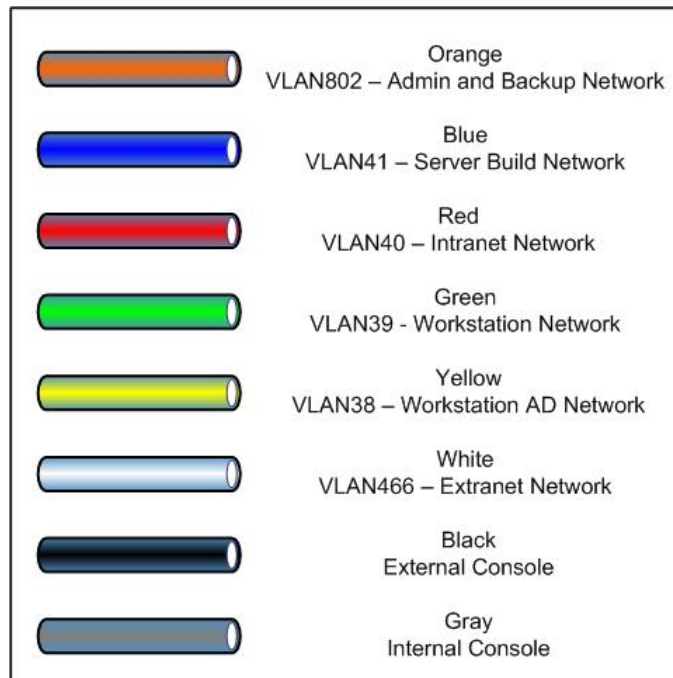


Figure 3 – Ethernet Cable Color-Coded Scheme

SEF VLANs:

- Admin and Backup Network (VLAN802)
- Server Build Network (VLAN41)
- Private (Intranet) Network (VLAN40)
- Workstation Network (VLAN39)
- Workstation AD Network (VLAN38)
- Public (Extranet) Network (VLAN466)
- External Console Network
- Internal Console Network

Admin and Backup Network

The purpose of the Admin and Backup network is to provide administrative access to SEF servers as well as backup and restore services to the SEF with Symantec (Veritas) NetBackup.

Server Build Network

The purpose of the Server Build network is to provide a staging area where servers and other hardware are built and configured. These systems must be patched and security scanned prior to being moved to other SEF networks. The SEF Jumpstart and Kickstart systems are located on this network.

Private (Intranet) Network

The SEF Private network is used to host servers and other hardware to support SEF testing. Custom and COTS applications servers reside on this network in addition to the SEF Active Directory.

Workstation Network

This network consists of standard ODIN Microsoft Windows and Apple Macintosh workstations. These workstations are configured with ODIN core loads. The purpose of this network is to host user workstations. Often, these workstations are used to test against servers on the SEF private network.

Workstation AD Network

This network is for workstations that require access to Headquarters Active Directory Services. These workstations are running an ODIN core load.

Public (Extranet) Network

This network consists servers that require access from systems located externally to NASA HQ. This permits users from other NASA Centers or on the Internet access to these services for testing.

Console Networks

The purpose of the SEF Console Networks is to allow network-based access to the console of systems on the SEF network. Access is controlled by logging into a bastion host for these networks. Goin (Private) and Goout (Public) are located on these networks.

5. SEF Inventory

The SEF inventory is maintained so that it resembles the production environment as closely as is reasonable.

5.1 Inventory Maintenance

The SEF strives to maintain hardware, software, network devices, and other resources necessary to support testing requests. SEF hardware is maintained in an as needed inventory and scheduled and allocated as needed. The SEF environment is dynamic in that it often changes, but consistently maintained to support SEF and HQ functions. New hardware and resources are procured on an as needed basis when new testing requirements are identified and cannot be supported using existing SEF equipment.

The SEF personnel have access to the ODIN software library and may request NASA site licensed software for use in the SEF. Appendix C provides a listing of SEF hardware and software assets.

SEF equipment is either tagged or bar-coded for inventory control purposes. The SEF Managers document and manage equipment serial numbers, specifications and configurations for each device on hand for service calls and upgrades. The retirement process for SEF hardware is explained in section 6.6.

5.2 Logistical Support

The SEF environment remains dynamic such that it must be able to respond to changes in the NASA Headquarters Computer Center (NHCC) and Network Operations Center (NOC). Changes are also driven by ODIN desktop deployment strategies that may

require routine upgrades or refreshes of ODIN desktops within the SEF.

When applicable, hardware and software maintenance contracts are procured for some hardware assets such as servers located in the SEF. Other assets such as workstations are supported by the ODIN contract under the ODIN Seat definition (Table 3).

SEF Testing Workstations				
Location	Make	Model	OS	Coreload
Posits 1, 3, 4, 7, 9, 21, 23	Compaq	d530	Windows XP	Q35
Posits 2, 5-7, 18-20, 22	Apple	G5	OS 10.4	Q35

Table 3 – ODIN workstations

Currently, the SEF has thirteen workstations available as test pool devices (7 Intel and 6 Macintoshes). ODIN provides these workstations for testing purposes such as applications testing and core load testing. These ODIN workstations are kept within the ODIN lifecycle in order to reflect what the customer is currently using.

The volume of testing being conducted in the SEF determines the number of ODIN workstations needed in the SEF. Currently, the SEF maintains adequate ODIN workstation resources to meet typical testing volume. If a situation arises where the SEF does not have adequate ODIN workstations, a request could be made to ODIN for additional resources.

6. SEF Operations, Procedures and Testing

This section outlines the process through which applications, products and systems are evaluated and tested. A resource scheduling process is maintained by the SEF Manager based on needs identified through formal requests that are submitted by users. Requests to use the SEF are funneled through the SEF Managers. This procedure will ensure that all requests are treated as equitably as possible and that the lab's resources are not over-taxed. The SEF testing request process is discussed in further detail in Section 6.1.1.

6.1 SEF Operations, Scheduling and Resource Management

The testing of applications, products and systems in the SEF is initiated using a Task Management System (TMS). This web-based system along with a FileMaker tool assists SEF Managers in managing:

- SEF Testing Requests
- Task and testing lifecycles
- IP assignments
- Hardware inventory
- Backup and recovery images
- Reports and usage statistics
- Configuration management

6.1.1 Scheduling and SEF Availability

The goal of scheduling testing within the SEF is to accommodate all testers and SEF users as quickly as possible and maintain the integrity of the test environment. The SEF typically operates on a First Come First Served (FCFS) scheme for allocating resources. However, SEF scheduling is flexible to accommodate priorities. For example, a test may need to be immediately scheduled to resolve an anomaly that is occurring in production. This test may delay ongoing SEF testing that is not having an immediate production impact. The SEF environment is robust enough to normally support numerous parallel testing efforts. More details about SEF scheduling and availability is addressed in the sections that follow.

6.1.2 Test Request Process

The purpose of the test request process is to ensure that the appropriate hardware and software assets are configured and available when required and to avoid potential resource availability conflicts. The test request process also facilitates in providing a quality test environment for improvement and reliability of systems and applications to the NASA Customer..

Test requests are required when developers or engineers build or modify an application or system that needs to be tested for deployment. This process involves the allocation and scheduling of resources for testing purposes and the release of those resources when testing has been completed.

The following organizations, departments or positions provide inputs required for the process:

Software developers - Web enabled applications, client server applications, or any isolated desktop applications. Test plans that include full regression testing of applications to verify compatibility with existing NASA custom applications.

Engineering - Provide IT Standards/Procedures for performance testing both stress and scalability. Write compatibility, functionality, and quality assurance documentation. Assist with Test Plan development and ensure project requirements are satisfied.

Contractors - Provide hardware/software products to be tested in SEF. This will include reason for testing, application requirements, and will have an assigned Engineer to oversee testing performed.

NASA HQ - Products that need SEF testing for NASA Employees to verify they meet all requirements before deployment within NASA HQ.

The first step in the test request process is for the requestor to contact the SEF for inquiring about testing, equipment and software required, dates needed and any other requirements for assistance that may be needed. Next, the SEF manager will advise the User to go to the SEF TMS website at

http://vikings1.indyne.hq.nasa.gov/sef_tms/test_request.cfm and fill out a SEF Work Request. A sample SEF Work Request form can be viewed in Appendix D.

Upon receipt of the SEF Work Request, the SEF Manager will review the request to ensure that the scope of testing can be accommodated with existing SEF hardware and software assets.

When a test requester submits a test request to the SEF for evaluation, the SEF staff will begin their review of the criteria by evaluating the request form and identifying:

- Hardware or software availability
- Application or system version
- OS type and version
- Additional criteria such as network requirements and printer access.
- Scheduling availability
- Test plan requirements

Appendix E illustrates the process flow for the SEF Test Request Process.

After the review and based on asset availability, the SEF Manager will either approve or reject the test request or work with the test requester to determine the required testing environment. The SEF Manager will send voicemail or email (or in person) confirmation of the Systems Engineering Facility (SEF) Work Request receipt and clarify that the SEF will be ready or if a change is required, pending receipt of the test plan. The SEF managers will have the resources setup, labeled and ready for testing.

The requestor then begins testing according to the test plan, documents the test results and notifies the SEF when testing has been completed. When the SEF Managers receive notification that testing has been completed, the refresh cycle begins.

6.1.3 Test Plan Process

Developers, engineers and other testers must submit a test plan to the SEF for review prior to conducting a test. The test plan will describe the objectives, focus, scope, approach, and step-by-step process of the testing effort. The test plan is the benchmark by which the test results are evaluated.

The SEF Managers will review the test plan to point out any known issues or problems and to ensure all relevant data is collected. After the test plan is reviewed by the SEF Managers, notification is sent to the tester that they can proceed with their testing.

6.1.4 Developer and Government Testing

Developer and Government testing is the formal testing of a pre-production application or system by the customer. The testing process is documented in the SEF and noted under Section 6.1.2.1 and Section 6.1.3.

6.1.5 Test Completion and Documentation

Once testing has been completed, the tester shall document the results of the testing and

provide this information to the SEF Managers. The requestor shall also notify the SEF Managers when testing is complete so that SEF resources can be released for other testing requests. The tester must be prepared to demonstrate a final test with the SEF Managers of a successful and working product for deployment.

6.1.6 Innovation and Prototype Lab

The fundamental concept of the Innovation and Prototype lab is to provide an environment that fosters innovation and prototyping.

“Innovation involves deliberate application of information, imagination and initiative in deriving greater or different value from resources, and encompasses all processes by which new ideas are generated and converted into useful products”.¹
It may be either an incremental or revolutionary change in thinking, products, processes, or organizations.

A prototype creates or simulates a few aspects or features of the envisioned final solution, and may be completely different from the eventual implementation.

The goal is to test and evaluate new technologies. In addition, test and evaluate hardware, software and procedures that may not have been implemented at NASA or within the CIO community and possibly not tested, implemented or evaluated within the commercial IT community.

Within the existing physical and operational constraints of the SEF an Innovation and prototype lab will exist that will, to the maximum extent possible, enable agility in responding to requests from NASA. The goal is rapid turnaround with a minimum amount of paperwork.

The overall goal of the Innovation and prototype lab will be to increase the agility and timelessness in evaluating products, determining the applicability of solutions, vetting requirements, testing prototypes and procuring items in support of these activities and being more innovative in IT.

An example of a prototyping effort would be a quick turn around to determine if there is value in going forward to a pilot phase or make a recommendation if the initiative warrants more effort to move forward for production implementation.

Additional activities within the Innovation and Prototype Lab would be vendor technology briefings and brown bag and brainstorming sessions.

Much of the culture within NASA HQ IT is highly process driven with extreme adversity to risk. The culture of the Innovation and Prototype Lab should foster innovation, creative thinking and provide a “safe” environment where solutions can be evaluated without negatively impacting NASA production, development or test systems.

¹ <http://www.businessdictionary.com>

Staffing:

It is anticipated that the existing SEF staffing (SEF manager) will be responsible for the overall operation of the Innovation Lab supported by the HITSS Engineering department.

It is also anticipated that the current level of staffing will be adequate to manage and operate the Innovation lab.

However, if the level of requests submitted to the Innovation lab can not be handled with current staffing levels or if the level of requests have the potential to negatively impact contract metrics, staffing levels would need to be increased or a mechanism to throttle Innovation Lab requests will be examined.

Initiating an Innovation lab request:

It is anticipated that 3 mechanisms can be used to initiate a request for work within the Innovation Lab. All three of these mechanisms are currently in use today for general SEF work requests.

- 1) Open a Class 2 Service Request (SR)
- 2) Initiate a SEF testing request form.
- 3) An email from the NASA ITC&D Engineering manager to the HITSS Engineering manager

Hardware and Software:

It is not anticipated, at this time, that any new large Hardware or Software procurements will be required to support the Innovation Lab. The Current SEF assets are sufficient for the general support of the Lab. Small hardware or software procurements should be handled within the normal procurement processes without requiring specific SRs. However, for specific tests, evaluations or prototypes, new hardware or software may be required. Often these assets can be obtained on a temporary loan basis from vendors for a limited duration in support of product evaluation.

If hardware or software procurements are required, this would follow the normal procurement / approval process.

6.2 Lifecycle of SEF (Hardware) Assets

SEF servers and most non workstation SEF assets are classified as semi-permanent or transitory.

6.2.1 Semi-Permanent Assets

Semi-permanent systems are those servers or assets that remain with stable configurations within the SEF environment for extended periods of time and are available for testing or use at almost any time. Semi-permanent systems often mimic specific production servers or systems. Semi-permanent systems often span multiple testing efforts. Semi-permanent systems are those systems that are used often enough that it

would not be practical or cost effective to build on an as needed basis. Semi-permanent systems are often used by a known or defined group of testers on an ongoing basis. Semi-permanent systems often require testing scenarios to be implemented on an immediate basis. Semi-permanent systems are those systems that if built on an as needed basis would negatively impact testers, testing schedules or SEF user satisfaction. Some semi-permanent systems are those systems that a specific customer or task order is willing to fund for their exclusive use.

6.2.2 Transitory Assets

Transitory SEF servers or assets are those servers or assets that are built or configured on an as needed basis for a specific testing effort and or for a specific time interval. After the specific test or testing interval is complete, transient assets are repurposed for a different testing effort.

6.2.3 Asset Life Cycle Conclusion

While it is the goal of the SEF to have as many servers or assets classified as transitory in order to maintain the least number of servers within the SEF facility there is a competing goal to have testing assets available to all those who require them with the absolute minimum possible delay in testing asset availability.

While there is no contract metric for server or asset availability within the SEF environment, as there is in the production environment, there is a contract deliverable that “The SEF is available and configured to meet the **requestors**’ requirement(s)”

6.3 SEF Server and Workstation Refreshes

When testing cycles are complete, these systems, except for semi-permanent SEF systems, enter a refresh cycle so that they can be allocated for another task. This refresh process is described in greater detail in the sections that follow.

6.3.1 Workstation (ODIN) Refresh Process

When testing has been completed on ODIN workstations in the SEF, the SEF staff refreshes these machines with a copy of the ODIN core load.

The SEF workstation image refresh process begins when the SEF manager is notified that testing has been completed and the resources are no longer needed. A DVD core load refresh installer is provided by ODIN. The installer automatically erases the hard drive and configures the device with the core load.

NOTE: *ODIN supplies the SEF with current core loaded DVDs after they are approved and available for distribution. These core loaded workstations are kept within the ODIN lifecycle in order to reflect what is currently being used by the customer.*

6.3.2 SEF Server Refresh Process

The SEFs goal is to use automated system refresh tools in order to minimize human error and minimize the time required to refresh and repurpose systems. Unix Systems are

refreshed using either Jumpstart for Solaris systems or KickStart for RedHat systems. Windows systems are refreshed with ghosted images or manually if required. Systems can also be quickly recovered from tape by using the SEF Quantum I500 and NetBackup. Tapes and catalogs can be moved from the production NetBackup environment to the SEF when needed to support specific troubleshooting or rebuild efforts.

6.3.2.1 JumpStart Service

Solaris JumpStart has been deployed at HQ to automate server provisioning for Sun systems. See the JumpStart SOP at



for more detail

Engineering or Operations initiates a JumpStart for new systems as part of the SR or change request process. Engineering or Operations builds the server on the build network and depending on the application, Engineering, Operations or Applications Development installs the application. Systems are then security scanned and moved to the appropriate SEF network for testing.

6.3.2.2 Kickstart Service

The Red Hat Enterprise Linux (RHEL) OS has now been standardized and is being utilized for deployment of new services at NASA Headquarters. Due to the flexibility of the OS to be installed on multiple platforms, it is expected that deployments of RHEL will expand and increase. For that purpose, a similar service to the Solaris JumpStart system for automating installations has been developed for RHEL called Kickstart. Process and procedures for a Kickstart are the same as for Solaris build outs (reference section 6.3.2.1).

The Red Hat Enterprise Linux Version 5 Build Guide Revision 2.01a is the current version of the baseline build and should be referenced for either a manual or an automated build. The Kickstart service is still in its initial phases and should be considered a “work in progress”. As new services are introduced using the Red Hat OS, the Kickstart service will be enhanced and expanded accordingly.

6.4 SEF System Backup and Recovery

The SEF has a backup network that provides backup and recovery services to servers in the SEF using Symantec (Veritas) NetBackup. When data on a system needs to be backed up, the system is connected to the SEF Backup Network, the NetBackup client is installed and NetBackup is used to backup the system to the SEF Quantum I500 tape library.

6.5 System Migration from the SEF to the NHCC

A security scan must be performed and any security issues mitigated before moving systems from the SEF to the NHCC. A Systems Description Document (SDD) is required for new hardware deployments and a Version Description Document (VDD) for new applications. A security review and a completed deployment checklist must also be submitted prior to deployment.

6.6 Phase-out or Retirement of SEF Hardware

The effectiveness and efficiency of SEF servers and workstations must be continuously evaluated to determine when the product has met its maximum effective lifecycle. Considerations for retiring SEF systems include: Continued existence of operational need, matching between operational requirements and system performance, feasibility of system phase-out versus maintenance, and availability of alternative systems.

The phase-out of older systems requires that the SEF Manager open a ticket via Check-In, Check-Out (CICO). This ticket should include information about the system such as the make, model and property ID number.

Production data that reside on SEF systems exists solely for testing purposes and may not be copied and removed from the NASA HQ building. SEF systems that contain production data or sensitive application software must be removed by a NASA approved technique prior to removal from the premises. This process is described in further detail in Section 7.2.

6.7 SEF Configuration Management

The purpose of configuration management in the SEF is to monitor and track configuration changes applied to SEF servers and workstations. The SEF utilizes a configuration log that is maintained and updated on a daily basis.

Every day the SEF receives the current CR Log from production. The log is reviewed to determine what changes are needed in the SEF. For example a patch that will be going into production needs to be tested into the SEF first.

6.7.1 SEF System Update Management

Currently, the update and patch process for both the SEF and Production is a manual process. The goal is to automate this process as much as possible in the future. Patching is handled by a process outside the scope of the SEF because this incorporates Development and Production. The HQ patching process is currently in the process of being formalized. The SEF will provide integral support to defining this process.

When updates are applied and installed in the SEF applications are regression tested to verify that there is no impact. If the testing is successful, the update remains on the system. If the testing was not successful, the installation of the update is rolled back to restore the system to its previous state.

6.7.1.1 Windows Updates

Windows servers on the SEF Private network are updated from the SEF Windows Server Update Services (WSUS). The server is responsible for synchronizing with the Microsoft Update servers, providing those updates that are approved for clients in the SEF. The clients are responsible for querying the SEF WSUS server to see if there are new updates available. The SEF staff manually pushes these updates and validates the installation.

These updates are coordinated with Server Operations, such that these updates are tested in the SEF prior to being installed in production.

6.7.1.2 Solaris Updates

Sun Solaris systems in the SEF are updated manually using the latest patch cluster plus any additional patches deemed necessary. These updates are coordinated with Server Operations, such that patches are tested in the SEF prior to being installed in production.

Engineering and Operations build System V packages for Solaris servers on an as needed basis. This process is initiated by an event such as a new version of software or the need for a new application. For example when RSA issued a security fix for the pam module a new package was created.

6.7.1.3 RedHat Linux Updates

RedHat systems in the SEF are updated manually using RHEL YUM package updater. These updates are coordinated with Server Operations, such that patches are tested in the SEF prior to being installed in production.

6.7.1.4 Macintosh Updates

Macintosh servers in the SEF are updated manually and tested for compatibility. The updates are coordinated with Server Operations, tested in the SEF, then deployed to Macintosh servers in production.

7. Security Controls in the SEF

To ensure adequate security controls are in place, the SEF maintains appropriate controls as detailed in the SEF IT Security Plan. The SEF is comprised of two distinct security boundaries as follows:

Network	FIPS Data Impact	IP Space
SEF Admin Network	Moderate	
SEF Development Network	Low	

Table 4 – SEF Security Boundaries

The SEF Network is logically located within the security boundaries of the NASA HQ Private Network System Security Plan and inherits NIST 800-53 moderate security controls from the overarching security requirements satisfied by the security plan. For example; physical, logical and environmental controls have been implemented, certified and accredited on all SEF systems per the NASA HQ Private Network System Security Plan. In addition, technical and continuous monitoring controls such as configuration management, audit trails, risk assessment etc., are assessed at least annually or as needed to ensure compliance with the NIST 800-53 moderate security control set.

SEF Admin Network

The SEF Admin Network is logically located within the NASA HQ Private Network System Security Plan and is certified and accredited for approved FIPS moderate (production) data types. The purpose of the SEF Admin Network is to allow developers

and development systems to stage production systems and interface with moderate production data types.

SEF Development Network

The SEF Development Network is logically located within the NASA HQ Private Network System Security Plan and is certified and accredited for FIPS low data types. The purpose of the SEF Development Network is to develop and test pre-production IT systems. The SEF Development Network does not house FIPS moderate data types nor does it interconnect with networks that process and store moderate data.

7.1 System Security Application Software

All ODIN core loaded Windows workstations in the SEF receive software updates from HQ SMS as required. All ODIN core loaded Macintosh workstations in the SEF receive software updates from the HQ LanRev server as required. Servers on the SEF Private and Public networks utilize PatchLink software for reporting.

7.1.1 Security Policies

The SEF network inherits policies from NASA HQ and Agency level policy as noted in the implementation detail of the NASA HQ Private Network System Security Plan. Implementation detail references policy resources such as the NASA HQ Rules of Behavior and NPD 2810.1a that define acceptable use governing the NASA HQ Private Network system.

7.2 Production Data and Removal Process

The SEF network consists of two separate and distinct security boundaries. The SEF Development Network is approved for low (non-production) data types only. Data from the SEF Development Network is disposed in accordance with NIST 800-88 guidance as prescribed by the NASA HQ Software Management Guide which places little or no restriction on the removal of FIPS low data types.

The SEF Administrative network is approved for Moderate (production) data types. Data processed and stored on the SEF Administrative network is disposed in accordance with NIST 800-88 guidance as prescribed by the NASA HQ Software management Guide which places restrictions on data removal for Moderate data types. Moderate data stored on SEF devices must be adequately encrypted and wiped from temporary storage devices or archived as mandated by Federal Information Processing Standards.

Solaris Disk Wiping procedure for SEF:

Retrieve the NHQscrub.pkg package from barsoom:/usr/local/jumpstart/pkgs/5.10 and add the package to the system.

For all disks that need to be wiped run a command like the following:

```
/usr/local/scrub-2.1/bin/scrub -p dod /dev/rdisk/c1t2d0s2
```

Note that the devices must be the raw device and the slice should be slice 2 to get the whole disk.

To see the man page for the utility issue the following command:

```
man -M /usr/local/scrub-2.1/man scrub
```

Following is the details on what a dod scrub entails:

The dod scrub sequence is compliant with the DoD 5220.22-M procedure for sanitizing removable and non-removable rigid disks which requires overwriting all addressable locations with a character, its complement, then a random character, and verify. Please refer to the DoD document for additional constraints.

NetApp Disk Wiping procedure for SEF:

NetApp 2050 cluster will be the backend storage for Oracle servers. The Gomeisa and Wasat Oracle servers will utilize NetApp 2050c NFS exports for mounting needed file system. All NFS exports will be designed based on separate aggregates and volumes. These volumes will be on two different controllers and two different schemes (PII and Non-PII). All volumes will be optimizes for NFS performance and with proper access controls. NetApp provides a licensable and DoD compliant disk sanitization feature which only can be run locally from Filer. After expiration of PII (NFS exports) testing underlying volume/aggregate will be destroyed, this will return related disk back to Filer Spare Pool. Those disk will be sanitize by following procedures:

```
#aggr status -r <PII_aggr1> (to show all underlying disk in aggregate that needs to be sanitized.)
```

```
#disk sanitize start <disk1> <disk2> <disk3> ....
```

7.3 PII / Privacy Data

On occasion PII/Privacy data may be required for use to support testing or problem resolution. If / when PII is brought into the SEF or installed on any SEF system, the use of this data shall be registered with the HQ Privacy Manager (Bryan McCall). Once testing/use has been completed this data is to be removed and notification provided to Bryan McCall that it has been deleted.

8. SEF Manager Roles and Responsibilities

The roles and responsibilities of SEF personnel are described in detail in this section.

8.1 SEF Manager

The primary role of a SEF Manager is to supervise the management and operations of the SEF. The SEF Manager is responsible for the overall operation of the facility, which includes management, monitoring, maintenance, and protection of all SEF equipment. The SEF Manager will need to develop realistic schedules for product and systems testing, working with project managers, engineers, and developers to merge testing schedules into overall project schedules. The SEF Manager will also investigate new technological developments to evaluate their potential advantages to the organization.

The SEF Manager monitors the lab's usage (number of products tested, number of users testing, resources utilization, etc.) on a monthly basis to help to manage user expectations and to provide statistical information to management for monthly in-depth reports.

Specific Responsibilities:

- Ensuring all evaluation and testing activities are performed consistent with this

Concept of Operations

- Scheduling and prioritization of SEF resources
- Receiving, reviewing and approving Testing Requests
- Primary point of contact for Testing interaction and evaluation
- Provide technical expertise to Testers and Users during the testing process
- Arranging and preparing testing environments
- Briefing Management on testing statuses
- Maintaining updates to the Facility policies and procedures
- Ensuring that appropriate mechanisms are in place to protect the interests of all parties
- Ensuring all Facility operations adhere to the security and confidentiality requirements
- Maintaining the integrity of SEF materials as well as following all applicable copyright laws related to software installations and upgrades
- Submitting monthly metrics to Management
- Managing internal networks and systems
- Acquisition, configuration, and updates to hardware

8.2 SEF Manager Core Skill Requirements

Experience and Requirements:

- Knowledge/experience with Internetworking devices such as switches, routers, access points.
- Knowledge/experience with patch panel and cable management.
- Expertise in cross-platform operating systems and computing platforms
- Familiarity with office productivity applications, such as e-mail, spreadsheets and databases.
- Experience in Systems Administration.
- Excellent verbal and written communication skills.
- Familiarity with operating systems and products deployed at NASA HQ.

8.3 SEF Users

There are various types of users that may request testing in the facility. A SEF user normally consists of one of the following:

- Systems engineers
- Network and system administrators
- Applications testers
- Application developers
- Database administrators
- Quality assurance specialists
- NASA civil servants, and contractors
- IT security

9. Recommendations

This section presents recommendations for improvements to the SEF infrastructure and or processes.

9.1 Process Improvement

SEF process will be improved continuously and proven improvements will be adopted. When possible and practical, relevant data will be collected for process improvement analysis.

9.2 Network Address Translation (NAT)

Eliminate the use of NAT with the SEF Extranet Network. The NAT configuration is confusing and unnecessary given that the network is protected with a firewall.

9.3 Developer Access

Establish the appropriate firewall rules that allow developers appropriate SEF access from the off-site facilities/locations without the requirement of VPN. This effort could be part of the initiative to move the HITSS facilities off of NASA address space.

9.4 Automated Patch Management

Implement mechanisms for automated patch management for both Red Hat Linux and Solaris that can be used to automate the process of patch management and deployment. After this is implemented and tested in the SEF the same mechanisms should be appropriate for production systems.

9.5 Research Bug Tracking Systems

Research bug tracking solutions and implement one that best matches requirements. The solution should be easy to use and help capture and track all relevant data related to an issue throughout the life cycle of the issue.

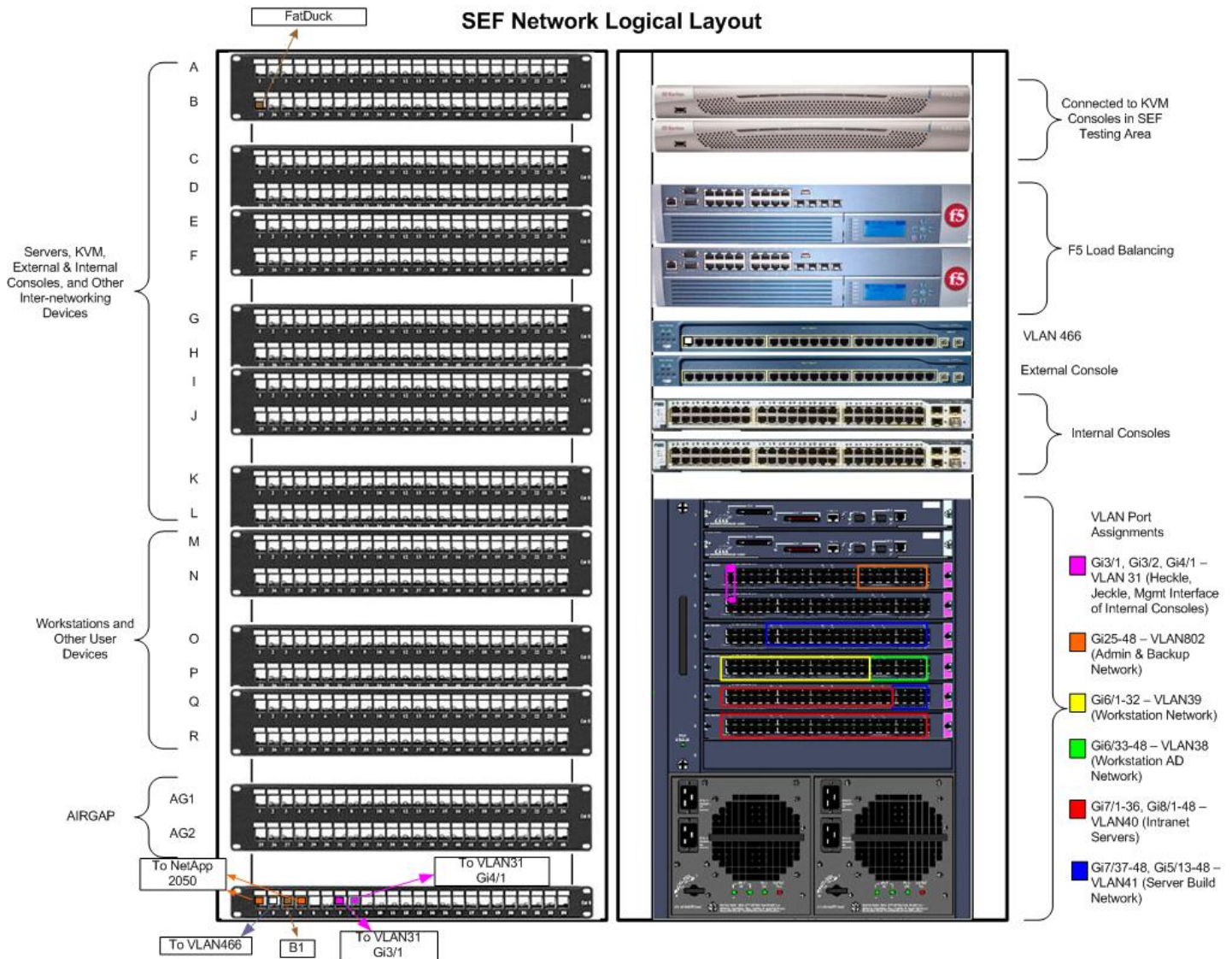
9.6 Develop Web Log for SEF CM Tracking

Provide a method by which developers and engineers can track SEF configuration management changes through the use of a web log. The solution should be searchable and provide for a history of all relevant changes over time.

9.7 Reorganize SEF Server Racks

Identify and reorganize SEF server racks to reflect the type of equipment such as Permanent and Pool.

Appendix A: SEF Patch Panel and Switch Layout



Appendix B: SEF Hardware Assets

Server Name	Make	Model	OS	Purpose	Type
accmonitor	DELL	2950	Windows W2k3 Server	Verifies web sites for accessibility and to programmatically fix errors. Verifies in W3C mode and Section 508 mode.	Pre-Production
bolide	DELL	2950	Windows W2k3 Server	Replicate SMDWEB1 and SMDWEB2	Pre-Production
converter	DELL	2950	Windows W2k3 Server	APPDEV Test box	Core Element
encase 1	DELL	1650	Windows W2k3 Server	Forensics	Test Pool
facilities ii	DELL	2950	Windows W2k3 Server	HQ Facilities test box	Core Element
hqpressman	DELL		Windows W2k3 Server	Printer Monitoring	Test Pool
netiq3	DELL	2950	Windows W2k3 Server	NETIQ Security Manager	Test Pool
netiq2	DELL	2950	Windows W2k3 Server	NETIQ Security Manager	Test Pool
netiq1	DELL	2950	Windows W2k3 Server	NETIQ Security Manager	Test Pool
patchlink	DELL	2950	Windows W2k3 Server	NETIQ Security Manager	Test Pool
sefdba	DELL	2950	Windows W2k3 Server	APPDEV Test box	Core Element
sefdc	DELL	2950	Windows W2k3 Server	SEF Domain Controller/AD	Core Element
sefbdc	DELL	1750	Windows W2k3 Server	SEF Backup Domain Controller and Archibus test box	Core Element

sefwsus3	DELL	2950	Windows W2k3 Server	UPDATE SERVICES	Core Element
sefteamtrackdev	DELL		Windows W2k3 Server	CHECK-IN, CHECK-OUT	Core Element
sefteamtrack	DELL	2600	Windows W2k3 Server	CHECK-IN, CHECK-OUT	Core Element
sefvlan41	DELL	2950	Windows W2k3 Server	SEF VLAN 41 Test Box	Test Pool

Server Name	Make	Model	OS	Purpose	Type
aramis	SUN	V240	SOL10	Artisia Primary	Pre-Production
arrakis	SUN	V210	SOL10	CENS	Pre-Production
athos	SUN	V210	SOL10	ArtesiaDAM	Core Element
barsoom	SUN	V210	SOL10	JumpStart	Core Element
caladan	SUN	V210	SOL10	CENS	Pre-Production
canopus	SUN	V210	SOL10	COGNOS Cold Fusion Testing	Core Element
corport	SUN	V210	SOL10	SMD - SpaceOps	Core Element
deneb	SUN	V210	SOL10	OEM	Pre-Production
dhcp2	SUN	V210	SOL9	DHCP	Core Element
dorado	SUN	V210	SOL10	Check-In Check-Out DB	Core Element
dynamite	SUN	V245	SOL10	HP OPENVIEW	Pre-Production
frack	SUN	V245	SOL9	NetIQ Agent Test Box	Test Pool
freefall	SUN	280R	SOL9	Exploration Systems	Core Element
frick	SUN	V245	SOL9	NetIQ Agent Test Box	Test Pool
gacrux	SUN	T2000	SOL9	NetBackup	Core Element
gomeisa	SUN	V240	SOL9	Intranet DB	Core Element
gomeisa2	SUN	V210	SOL9	Intranet DB	Core Element
goin	SUN	V210	SOL9	Bastion (internal consoles)	Core Element
goout	SUN	V210	SOL9	Bastion (external console)	Core Element
komi	SUN	V210	SOL9	POPs Dev	Core Element
marfak	SUN	V210	SOL9	DMS Application	Core Element
marib	SUN	V245	SOL9	ArtesiaDAM	Pre-Production
mekbuda	SUN	V240	SOL9	DMS DB	Core Element
netman1	SUN	V210	SOL10	Cisco Works	Pre-Production
obelisk	SUN	X4100	SOL9	Bianca Dev Box	Core Element
octans	SUN	V240	SOL9	Focus DB	Core Element
phred	SUN	V210	SOL9	Nagios	Core Element
picis	SUN	V210	SOL9	Focus Applicaton	Core Element
porrima	SUN	V210	SOL10	Extranet WebApp	Core Element

procyon	SUN	V210	SOL9	Intranet WebAPP	Core Element
procyon2	SUN	V210	SOL9	Intranet WebAPP	Core Element
rawhide	SUN	V210	SOL9	E-mail Routing System	Core Element
redsage	SUN	V210	SOL10	Working Group Respository	Core Element
remington	SUN	V245	SOL10	Crystal Reports (Private)	Core Element
river	SUN	X4200	SOL9	Virtual - Master Site Redesign	Test Pool
rotanev	SUN	V210	SOL8	Crystal Reports	Core Element
ruger	SUN	V245	SOL10	Crystal Reports	Core Element
sagitta	SUN	V245	SOL10	ARMD	Core Element
scout	SUN	V210	SOL9	Packaging	Core Element
sham	SUN	V245	SOL10	ARMD	Core Element
silver	SUN	V210	SOL10	Packaging	Test Pool
spica	SUN	V240	SOL10	Extranet DB	Core Element
spinoza2	SUN	V210	SOL9	List Server	Core Element
tabit	SUN	V210	SOL10	Netbackup Client	Test Pool
thuban	SUN	V240	SOL9	Netbackup	Core Element
thunder	SUN	V210	SOL9	ARMD, Cumulus	Core Element
trithemius	SUN	VV100	SOL9	Forensics	Test Pool
trigger	SUN	V210	SOL9	Plone	Core Element
vega	SUN	V210	SOL10	Brio	Core Element
vela	SUN	V210	SOL10	DMS for SPOs	Test Pool
vihlma	SUN	V210	SOL10	Simplicity Testing	Test Pool
watchtower	SUN	V210	SOL9	RSA SecureID	Core Element
woodbridge	SUN	X4100	SOL9	SMB	Core Element
fatduck	SUN	X4200	SOL10	POPs	Core Element
muliphen	SUN	V210	SOL9	DMS DB	Core Element
murzim	SUN	V210	SOL9	DMS APP	Core Element
porrima2	SUN	V210	SOL8	Extranet Webapp	Core Element
propus	SUN	V210	SOL9	BRIO App	Core Element
ruchba	SUN	V210	SOL8	Crystal Reports	Core Element
spica2	SUN	V210	SOL8	Extranet DB	Core Element
wasat	SUN	V240	SOL9	BRIO DB	Core Element

Server Name	Make	Model	OS	Purpose	
cards	DELL	1650	REDHAT ENT 5	DRNO	Test Pool
satellite	DELL	2850	REDHAT ENT 5	RedHat Kickstart	Core Element
leonis	SUN	X4100	REDHAT ENT 5	KickStart Dev System	Core Element
satellite	DELL	2850	REDHAT ENT 5	RedHat Satellite System	Core Element
springfield	DELL	2950	REDHAT ENT 5	Subversion	Core Element
winchester	DELL	2950	REDHAT	Subversion	Core Element

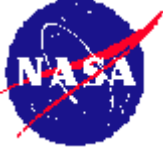
			ENT 5		
mauser	DELL	2950	REDHAT ENT 5	NETIQ Dev System	Core Element
walther	DELL	2950	REDHAT ENT 5	Entellitrak Dev System	Core Element
beretta	DELL	2950	REDHAT ENT 5	Red Hat Dev System	Core Element

Server Name	Make	Model	OS	Purpose	Type
seffm1	APPLE	XSERVE	10.3	FileMaker Pro Server	Core Element
cumulussef	APPLE	XSERVE	10.3	Cumulus Server	Core Element
sefxserveg5	APPLE	XSERVE	10.4	SEF Test Box	Test Pool
lanrev	APPLE	XSERVE	10.4	LANREV Test Server	Core Element
seftiger	APPLE	XSERVE	10.4	Mac OS Test Server	Test Pool

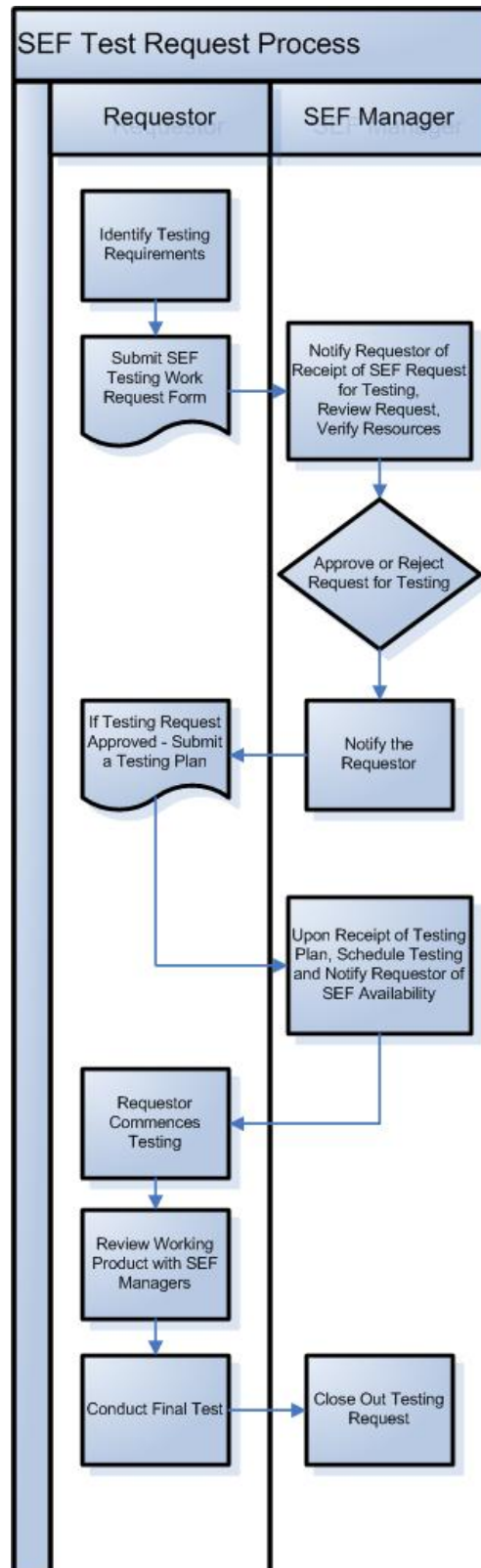
Name	Make	Model	OS	Purpose	Type
CISCO 3600	CISCO	3600		Router for Encase1	Core Element
ADIC i500	ADIC	i500		Tape Box for NetBackup	Core Element
Juniper		4000		Secure Access Lab Unit	Core Element
F5				Load Balancing	Test Pool
F5				Load Balancing	Test Pool
F5				Load Balancing	Test Pool
F5				Load Balancing	Test Pool
XRAID	APPLE			Raid for SEFFM1	Core Element
XRAID	APPLE			Raid for Cumulus	Core Element
XRAID	APPLE			Raid for SEFTIGER	Test Pool
SEFPriter	Xerox	5030		SEF Printer	Core Element

Software	Platform	Version	Owner	Purpose
System Core Load	PC	Q36	ODIN	Standardized Windows load for all ODIN desktops
System Core Load	Macintosh	Q36	ODIN	Standardized Apple load for all ODIN desktops
Windows 2003 Server	INTEL	Standard	HITSS	Server Software
Windows 2003 Server	INTEL	Enterprise	HITSS	Server Software
Solaris 9	SUN/Intel	9	HITSS	Server Software
Solaris 10	SUN/Intel	10	HITSS	Server Software
RedHat Linux	SUN/Intel	4	HITSS	Server Software
RedHat Linux	SUN/Intel	5	HITSS	Server Software
Macintosh OS X	Apple	10	HITSS	Server Software

Appendix C: System Engineering Facility (SEF) Work Request Form

		SYSTEM ENGINEERING FACILITY (SEF) WORK REQUEST			
1. Name:		2. Phone:		3. Code:	
4. Date:		5. Type of Request:		6. SR or PR No.:	
7. Requestor:		8. Title:			
9. Description of work required:					
10. Type of Board Review (CCB, ORR) & Date:					
11. Requested completion date:		12. Total estimated hours:		Last Day of Testing:	
13. List hardware requirements (Mac or PC platform, scanner, Zip drive, etc.):					
14. List software requirements (OS version, application versions, etc.):					
15. List additional support needed (printer connection, etc.):					
16. Will this SR/PR result in installation/deployment on more than on NASA Code?			17. Which NASA Codes?		
18. Will successful testing result in baseline change?			19. Will there be concurrent users? If so, how many?		
20. List additional instructions:					
21. CCB or Manager approval (required for testing Custom, COTS, and GOTS applications, operating systems, and/or new hardware):					
<p>Please give at least a 24-hour notice when submitting your request.</p> <p>By signing this form, you understand that you are authorized to use only the above equipment for the task specified. Signature _____</p> <p>Emergency requests (requests made under 24 hour notice) must be approved by Ed Motsinger.</p> <p>SEF Manager Approval: _____ Date: _____</p>					

SEF Form June 07 Previous Editions Are Obsolete.

Appendix D: SEF Test Request Process

Appendix E: Acronyms and Abbreviations

COTS	Commercial Off-the-Shelf Software
FCFS	First Come, First Serve
GOTS	Government Off-the-Shelf Software
HQ	NASA Headquarters
NAT	Network Address Translation
NHCC	NASA Headquarters Computer Center
OS	Operating System
SDD	System Description Document
SEF	Systems Engineering Facility
VDD	Version Description Document
VLAN	Virtual Local Area Network
VPN	Virtual Private Network